

第9回

VPN

VPN運用のポイントを知る

VPN(Virtual Private Network)は、インターネットなどのオープンなネットワーク上でセキュアな通信を可能にする技術だが、あくまでもデータ通信の安全性を保証するものではない。つまり、VPN通信を行うマシンや、それを利用するユーザーに対する安全性は保証されておらず、VPNを用いる際はこれらに対して、何らかのセキュリティ対策を施す必要がある。そこで今回は、VPNをより安全に利用するため、運用時に留意すべきポイントについて解説する。

内藤正規
ネットワシシステムズ



アクセス・コントロールを構成する3つの要素

VPNでは通常、データの暗号化とカプセル化(IPアドレスなどのヘッダ情報を付加)により、セキュアな通信が可能となっているが、通信元と通信先のマシン自体の安全性は確保されていない。

例えば、中央拠点に設置されたVPN機器と、リモートのホスト(自宅や外出先など遠隔地にあるマシン)との間の通信を実現する「リモート・アクセスVPN」を介して、リモートのホストからウイルス/ワームを送りつけられても、VPN機器はそれを防ぐことはできず、VPN機器に接続しているネットワーク上のマシンにウイルス/ワームが感染する可能性がある。つまり、VPNを介してデータを共有するということは、通信元と通信先のマシンにおいてセキュリティ上のリスクを共有することにもなるのだ。

こうした問題を解決する手段の1つとして、アクセス・コントロール(注1)という機能の採用が考えられる。この機能を利用することで、VPN機器だけでなく、VPN通信の安全性も確保できる。

アクセス・コントロールは、「認証」と表されることが多いが、厳密には「AAA」と略される「認証(Authentication)」「認可(Authorization)」「利用記録(Accounting、注2)」という3つの要素から構成されている。以下、アクセス・コントロールの3つの要素について順番に説明する(図1)。

認証

アクセス・コントロールの第1関門として大きな役割を担うのが認証という処理であり、ここではアクセス

してきたユーザー/マシンの正当性を評価して接続の許可/拒否を決定する。一般的には、ユーザーのアカウント名とパスワードを基に正当なユーザーであるかどうかを判定する場合が多い。ここで、正当なユーザーであることが確認されれば接続が許可される。

パスワードの強度を高める方法としては、「パスワードを毎月変更する」といった人手による作業に依存する手法が挙げられることが多い。しかしながら、この手法はあまり効果的ではない。なぜなら、VPNによって通信の安全性は確保されているので、パスワードが傍受されるというリスクは無視できるからだ。にもかかわらず、この手法は、管理者にはパスワードの再設定や通知、ユーザーにはパスワードを記憶しなおすという作業を強い、管理者とユーザーの双方に大きな負担をかけることになる。しかも、パスワード変更作業の過程で情報が漏洩してしまうという危険も決して小さくはない。

同様に、パスワードを規定回数以上間違えたらアカウントをロック(注3)することで、保護するという手法もあるが、こちらも問題がないわけではない。この手法を用いた場合、アカウント名さえ入手できれば、故意にパスワードを間違えてログイン操作を繰り返すことで、そのアカウントの利用を一時的に停止さ

注1：アクセス・コントロールは、サーバへアクセスするユーザー/マシンを制御する機能。VPNに限らず、リモートのホスト(クライアント)からのアクセスを受け付けるマシン(サーバ)には必須の機能である

注2：AAAの要素の1つである「Accounting」は、「課金」という訳語が一般的に用いられているが、「利用記録」のほうが実際の処理や意味に近い。そのため、本稿では「利用記録」を訳語として用いている

注3：アカウントとはリソースを利用するための権利、または利用する際に必要なアカウント名(ユーザー名)/パスワードのことであり、アカウントをロックするとは一時的にアカウントを無効にすること。アカウントを無効にすれば、そのアカウントでリソースが利用できなくなる

せることができちゃうからだ。よって、この手法はVPN通信の停止が許されないユーザーには適用すべきではないだろう。

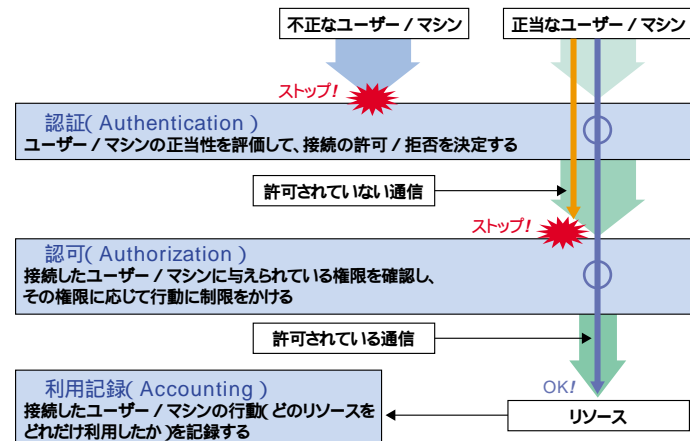
最近では、人手による作業に依存せずに認証精度を高める有効な手段として、バイオメトリクス認証(注4)が注目を浴びている。バイオメトリクス認証は、人間であるユーザー本人から切り離すことができず、かつ他人が持ちえない生体情報を用いて認証を行うため、現状、最も強力な認証方法だと見なされている。バイオメトリクス認証で利用可能な生体情報にはいくつかの種類があるが、現在のところは、指紋認証が操作性にすぐれ、誤認識(注5)が少ないため、普及が進んでいるようだ。なお、バイオメトリクス認証は、電子証明書と組み合わせて使用するのが一般的である。

認可

認証によって接続が許可されたら、次は認可という処理が行われる。この処理では、ユーザー/マシンに与えられた権限を確認し、その権限に応じてユーザー/マシンの行動に制限をかける。また、「利用は業務時間中のみ」1回の接続につき利用できるのは「時間」といった形で、接続時間に関する制限を設けることもできる。

一般に、通信に対する認可は、認証サーバで(権限ごとに振り分けられた)IPアドレスを基に制御したり、ネットワーク機器でパケット・フィルタリングしたりすることで実現される。ファイアウォール機能を備えたVPN機器ではこうした処理が行えるが、そうではないVPN機器では、リモートのホストに対するパケット・フィルタリング機能が十分ではないことが多く、さらには、ログが記録できないなどの問題があるケースも少なくない。したがって、リモート・アクセスVPNでの認可は、ファイアウォール専用装置で行うことをお勧めする。122ページの図2にVPN機器とファイアウォールの設置例(2種類)を、同ページの表1にそれらの長所と短所を示したので参考にしてい

図1: アクセス・コントロールの仕組み



ただきたい。

なお、ファイアウォール専用装置に加えて、IDS (Intrusion Detection System:侵入検知システム)を導入すれば、ウイルス/ワームの防御や、正当なユーザー/マシンによる不正な行動の監視が可能になる。

利用記録

認可の処理を受けてようやく通信可能になるが、その際は利用記録という処理が必要となる。利用記録はユーザー/マシンの行動を記録する処理であり、その記録を参照することで「だれが、どのマシンから、どのリソースを、どれだけ使ったのか」といったことが追跡できるようになる。

また、この記録は、リソースがどれくらい活用されているかを計るという点でも有用であり、リソースの過不足の検討資料にできる。加えて、障害が発生した際には、原因を解明するための材料にもなる。さらに、トラブルを巡って法的に争うようなケースで

注4: バイオメトリクス認証は生体認証とも呼ばれており、認証に用いることができる生体情報には指紋、掌紋、虹彩、静脈などがある。また、認証に生体反応を用いるものもあるようだ

注5: 誤認識は2種類ある。一方は正当な物を正当でないとして識別してしまうケースで、もう一方は正当でない物を正当と認識してしまうケースだ。認証において重視されるのは、後者の誤認識の少なさである



図2：VPN機器とファイアウォールの設置例

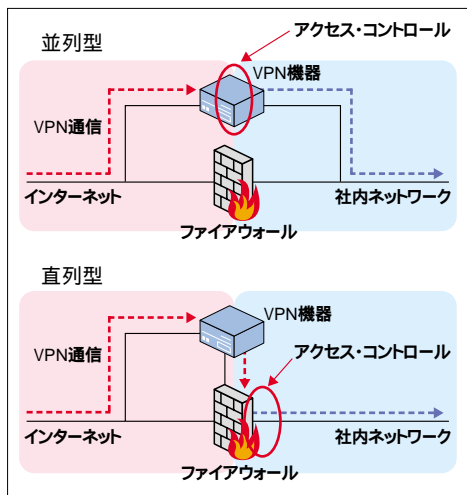


表1：VPN機器とファイアウォールの設置方法別の長所と短所

設置方法	概要	長所	短所
並列型	VPN機器とファイアウォールを並列に設置し、アクセス・コントロールはVPN機器が行う	VPN通信に対してのみ適用するフィルタリング・ルールを設定すればよいため、ルールを簡略化できる	強力なパケット・フィルタリング機能を備えていないことが多いため、セキュリティ対策が不十分な場合もある
直列型	VPN機器とファイアウォールを直列に設置し、アクセス・コントロールはファイアウォールが行う	プロトコルによるアクセス制限が行いやすいため、セキュリティ対策が強化できる。また詳細な通信記録が取れる	ファイアウォールを介すると通信できないプロトコルがまれにあるため、導入する前に調査する必要がある

表2：リモートのホストとユーザーに対するセキュリティ・リスク

攻撃対象	インターネット経由のセキュリティ・リスク	物理的なセキュリティ・リスク
リモートのホスト(マシン)	悪意のあるコンテンツ 情報漏洩 ネットワーク攻撃 ウイルス/ワーム 不正侵入および乗っ取り	盗難 / 紛失 悪意のある不正操作 操作ミス 不正なデータの入力
ユーザー	悪意による情報漏洩	ソーシャル・エンジニアリング 正当なユーザーによる情報の不正な利用

は、こうした記録がなければ、不当な不利益を受ける可能性もある。ITが自社のビジネスと深くかかわりあうようになった今日では、クレジットカードの利用控えを保管するのと同じように、リソースの利用状況を記録しておくことも重要なのである。

これらの3要素のうち、どの要素を欠いても安全なりモート・アクセスVPN環境を構築することはできない。そのため、いかなるVPN機器でも、何らかの形でこうした処理を行うための機能が実装されているはずだ。なお、アクセス・コントロールにより、有用な情報(ユーザー / マシンの行動)が記録できるのだから、それを活用しない手はない。したがって、製品選択の際には、情報の記録形式と、加工のしやすさについても吟味することをお勧めする。

インターネット経由のセキュリティ・リスクへの対策

リモート・アクセスVPNを安全に利用するための対策のうち、上述したアクセス・コントロールはサービスを提供する側(VPN機器)で行うものだが、サービスを利用する側(リモートのホスト / それを利用するユ

ーザー)でも安全性を確保するために何らかの対策を施し、セキュリティ・リスクを回避する必要がある。

リモートのホストと、それを利用するユーザーに対するセキュリティ・リスクには、インターネット経由のもの、物理的なものの2種類がある(表2)。そこでまずは、リモートのホストにおけるインターネット経由のセキュリティ・リスクと、それを防御するための手法について説明しよう。

スプリット・トンネルを悪用した攻撃

VPNが利用され始めた当初、リモートのホストが通信相手ごとに通信経路を切り替える「スプリット・トンネル」という機能を悪用した攻撃が、セキュリティ上の問題となった。スプリット・トンネル機能を有効にした場合、通信経路をVPNか、それともインターネットなどVPN以外のものかに切り替えることができるため、VPN以外の経路を利用したマシンが、不正侵入や乗っ取りの被害を受けたり、ウイルス/ワームに感染したりするケースがあるのだ。そうしたマシンがVPN経由で社内ネットワークに接続すると、そのホストが「踏み台」となって社内ネットワークが攻撃されたり、ウイルス/ワームが、社内はもとより社外にも広まったりしてしまう危険性が考えられる(図3)。

スプリット・トンネル機能を利用しなくても、通信をVPN経由に限定して行っていない場合、安全ではなく、「1ウェイ攻撃」(注6)を回避することもできない。こうしたインターネット経由のセキュリティ・リスクによる被害を防ぐために、VPNクライアントの中には、簡易なパーソナル・ファイアウォールが組み込まれたものも存在する。これを用いれば、リモートのホストに対する攻撃を防ぐことができる。

なお、リモートのホストのセキュリティ・リスクから社内ネットワークを守るには、やはりファイアウォールやIDSを配置することになる。最近のVPN機器の中には、そうしたリモートのホストからの攻撃を自動的に防御する機能を備えているものもあるので、その種の製品を選ぶのもよいだろう。

VPN機器によるリモートのホストの制御

VPN機器がリモートのホストからの攻撃を防御する機能を備えていたとしても、不特定多数のリモートのホストから社内ネットワークを守ることはきわめて難しい。そこで、認証を行う際に特定の条件を満たしていないリモートのホストを排除し、安全なホストのみVPN接続を許可するという仕組みが考え出された(図4)。

具体的には、VPNクライアント・ソフトがウイルス対策ソフトやパーソナル・ファイアウォールなどと連携して、リモートのホストをチェックした結果をVPN機器に通知し、その内容を基にVPN機器は接続の許可/拒否を判断する。さらに、認証時にパーソナル・ファイアウォールのルールを強制的に変更して、VPN接続の最中に不正な攻撃を防ぐこともできるようになっている。

また、リモートのホストはVPN接続中でも定期的にチェックされ、認証時には条件を満たしていたリモートのホストであっても、条件を満たさなくなったら強制的に切断される。こうした形での運用には、コストと労力を要するが、重要な情報の通信を行うならばこうした対策を講じるべきである。

図3：VPNのスプリット・トンネル機能を悪用した攻撃

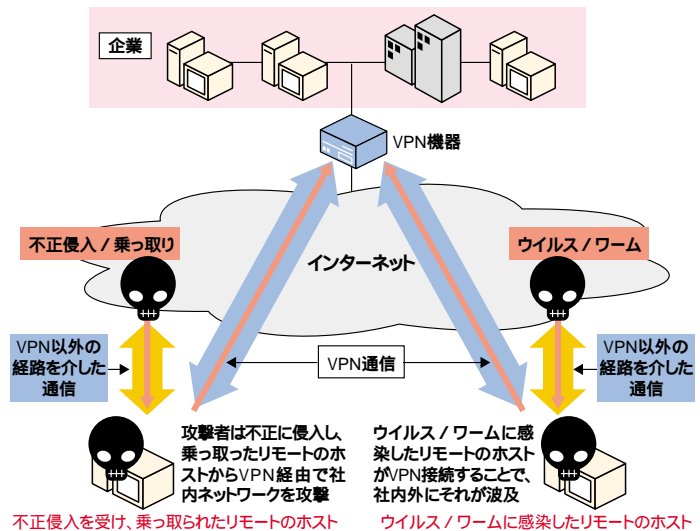
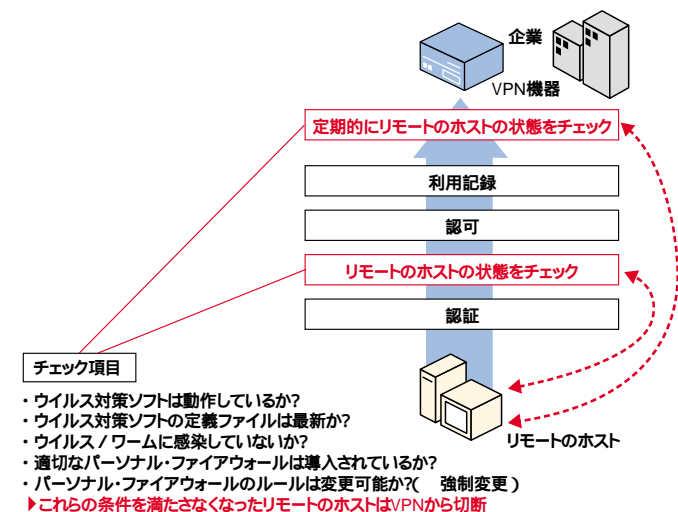


図4：リモートのホストの状態をチェックしてアクセスを制限



物理的な セキュリティ・リスクへの対策

次に、リモートのホストを取り巻く物理的なセキュリティ・リスクと、その対策について説明しよう。リモ

注6：1ウェイ攻撃とは、1つのパケットを送りつけるだけで成立する攻撃のこと。よって、この攻撃では、往復可能な経路が必要ない。昨年1月、マイクロソフトの「SQL Server 2000」の脆弱点を突いた「SQL Slammer」ワームが、この攻撃手法により猛威をふるった



ートのホストや、それを利用するユーザーが物理的なセキュリティ・リスクから守られていないかぎり、どんなに厳しいアクセス・コントロールを行っても、VPN通信の安全性は低下してしまうことになる。

物理的な乗っ取り

例えば、リモートのホストがVPN接続したままの状態では放置されたとして。この場合、接続時にアクセス・コントロールでユーザーを認証したとしても、認証を受けた本人がその場にいないければ、第三者がそのマシンから正当なユーザーの権限を悪用してVPN経由で社内ネットワークにアクセスできる。こうしたリスクに対しては、認証時にリモートのホストにスクリーン・ロック(注7)が設定されているかどうかをチェックすることで対応しているVPN機器もある。

正当なユーザーによる情報漏洩

VPNを利用するユーザーは、モラルを持って行動しなくてはならない。詳しくは後述するが、正当な権限を持ったユーザーにより正規に引き出された情報が不当に用いられた場合の対応は非常に難しい。この問題は、ユーザーに対してモラル順守の教育を行ったり、罰則を設けたりといったように、運用

時にフォローしていく以外にすべはない。

ソーシャル・エンジニアリング

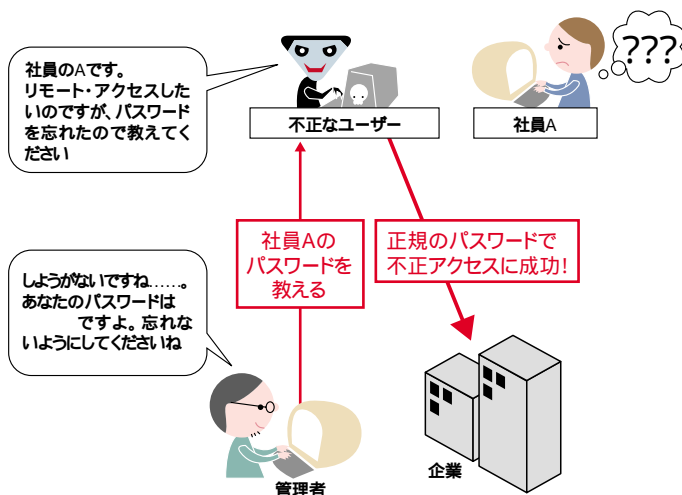
リモートのホストのセキュリティを強化し、ユーザーに対してモラル教育を行ったとしても防ぎづらいのが「ソーシャル・エンジニアリング」(注8)である。リモート・アクセスVPNでは、管理者とユーザー間で個人を特定する際に「視覚」を利用することができないため、ソーシャル・エンジニアリングを受けやすい(図5)。

ソーシャル・エンジニアリングは古くからある手法で、あきれるほど原始的だが、昨今流行している「オレオレ詐欺」に見られるように、時代を問わず有効な手法である。

なお、ソーシャル・エンジニアリングの典型例には、管理者が不正なユーザーにパスワードを直接教えてしまうことがあるが、パスワード自体を教えずに、それを類推できる情報を与えるだけで、まふと盗まれてしまう場合がある。こうした被害を防ぐためには、組織内でルールを決めて徹底するしかないだろう。

そのほか、セキュリティに関する教育が不十分だと、ユーザーは複雑なパスワードをメモ書きして保管してしまうことがある。そうした状況では、ガベージ・コレクション(注9)によって、機密情報が漏洩する可能性があるので注意されたい。

図5: ソーシャル・エンジニアリングの例



セキュリティ・ポリシーの重要性

ここまでの説明で、VPNの運用に際しては、たく

注7: スクリーン・ロックは、ある一定の時間、何も操作されなかった場合に、一時的にマシンの操作を行えなくする機能。再度、操作を行う際には、パスワードの入力が求められる

注8: ソーシャル・エンジニアリングとは、社会的な手段で何かを行うこと。ネットワーク・セキュリティ分野の用語としては、話術による聞き出し、盗み聞き、のぞき見などによって、重要な情報を収集することを指す

注9: ガベージ・コレクションとは、直訳すると「ゴミ集め」である。ネットワーク・セキュリティ分野の用語としては、悪意を持った人間がゴミ箱をあさってパスワードが書かれたメモなどを収集したり、個人情報(家族の名前など)が記載された書類からパスワードを推測したりしていたことから、一般に不用と思われるものから不正アクセスに有用な情報を得る行為を指す

COLUMN

どうする？ 私有PCからのリモート・アクセス

ノートPCの普及に伴って、企業では、ユーザーによる私有PCの持ち込みがネットワーク・セキュリティを脅かすものとして問題になっている。そもそも、私有PCを会社に持ち込むことは公私混同の行為と言え、大抵は禁止されているはずなのだが、不況の影響もあり、業務で使うノートPCの会社支給がままならないため、やむをえず私有PCが持ち込まれているのであろう。

企業に私有PCが持ち込まれると、さまざまな問題が発生する。1つは、運搬時に紛失や盗難にあった場合、そのPCに格納されている社内の機密情報が漏洩する可能性があることだ。また、最近では私有PCを通じて、ウイルス/ワームが持ち込まれるケースが頻発している。社内で万全なウイルス/ワーム対策を行っていたとしても、ウイルス/ワームに感染した私有PCが社内ネットワークに接続されることで、瞬間に感染が社内外に広がってしまう。

さらに、インストールするソフトウェアに制限のない私有PCに入っていたP2P (Peer-to-Peer) ソフトにより、機密情報が外部に流出してしまうことも考えられる。私有PCは業務用として企業から支給されているPCと異なり、セキュリティ・ポリシーを適用できないため、事実上、無法状態にあるといっても過言ではない。昨今、情報漏洩に対して厳重な対策が行われているなか、私有PCにより、社内の情報があっけなく持ち

出されるという事態は絶対にあってはならない。

VPNを含むリモート・アクセスでも、私有PCを社内ネットワークに接続できるようになっている場合、何も制限をかけていなければ、私有PCの持ち込みと同じ問題が起こる可能性がある。したがって、私有PCからのリモート・アクセスを認める場合は、私有PCに対しても、会社支給のPCと同様に、適切なアクセス・コントロールを行う必要がある。さらに、エンドユーザーへの十分な教育とVPN機器によるセキュリティ対策を行えば、セキュリティ上の問題の大部分は解決されるはずだ。

しかし、私有PCによるリモート・アクセスについては、セキュリティ以外の問題も存在する。それは、やはり公私の境界を曖昧にしてしまうという問題だ。具体的には、リモート・アクセス時の作業を就業時間として認めるかどうかといったことが挙げられ、労働争議にまで発展する可能性もある。それゆえ、私有PCによるリモート・アクセスの是非は結論が出ていないというのが実情である。

今後、ノートPCの利用は増えこそすれ、減ることはないだろう。よって、いつまでも私有PCの利用についてのルールを定めず、なしくずしに運用していくには限界がある。適切なリモート・アクセス環境を構築/運用するためには、セキュリティ・レベルとリモート・アクセスのバランスをじっくり考えようとして、自社に適した利用形態を模索していく必要があるだろう。

さんのセキュリティ・リスクが待ち構えていることを知っていただけたことと思う。そのため、VPNの利用ルールをセキュリティ・ポリシーとして整備しておくことが必須の作業となってくる。最後に、セキュリティ・ポリシーの重要性について説明して、本稿の締めくくりとしたい。

まず、企業において、重役の名をかたってソーシャル・エンジニアリングが行われた場合を考えてみよう。重役からの問い合わせとなれば、求められるまま重要な情報を教えてしまう可能性が高いのではないだろうか。実際、リモート・アクセスVPNを利用している企業では、このような地位を悪用したハッキングを受けることが少なくないという。

また、かたりではなくても、社内の有力者が権力を盾に要求を通そうとするケースもよくある。これがまかり通ると、どんなセキュリティ対策も意味を成さなくなってしまう。

これらのような、企業の役職制度や上下関係からくる問題を解決するためには、社内ネットワークを守り、VPNサービスを提供する立場のIT/IS部門に対してそれなりの権限を与える必要がある。企業によっては、IT/IS部門が組織上、役員直轄などの強い権限を持つことがあるが、これは一部のユーザーに便宜が図られることを防ぎ、全社員に対して一貫した運用体制を徹底する必要があるからだ。

その際に、運用のよりどころとなるのがセキュリティ・ポリシーである。上記のような問題も確固としたセキュリティ・ポリシーがあれば、合理的に対応することができるようになる。一般に、セキュリティ・ポリシーは役員名で策定・施行されるため強制力がある。最近、企業において、社員による情報漏洩事件が多発しているが、こうした事件に対する備えとしても、禁止行為や罰則などをセキュリティ・ポリシーとして定めておくことを強くお勧めする。

CW